

08/29/00
JC917 U.S. PTO

08-31-00

A
1c511 U.S. PTO
09/650712
08/29/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship Mariani et al.
Applicant Microsoft Corporation
Attorney's Docket No. MS1-579US
Title: Systems and Methods for Limiting Access to Potentially Dangerous Code

TRANSMITTAL LETTER AND CERTIFICATE OF MAILING

To: Commissioner of Patents and Trademarks
Washington, D.C. 20231
From: James R. Banowsky (509) 324-9256
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

The following enumerated items accompany this transmittal letter and are being submitted for the matter identified in the above caption.

1. Transmittal Letter with Certificate of Mailing included.
2. PTO Return Postcard Receipt
3. Check in the Amount of \$1,390
4. Fee Transmittal
5. New patent application (title page plus 24 pages, including claims 1-35 & Abstract)
6. Executed Declaration
7. 3 sheets of formal drawings (Figs. 1-3)
8. Assignment w/Recordation Cover Sheet

Large Entity Status ☒ Small Entity Status ☐

The Commissioner is hereby authorized to charge payment of fees or credit overpayments to Deposit Account No. 12-0769 in connection with any patent application filing fees under 37 CFR 1.16, and any processing fees under 37 CFR 1.17.

Date: 8/29/00

By:

James R. Banowsky
Reg. No. 37,773

CERTIFICATE OF MAILING

I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the below-indicated date. Any Express Mail No. has also been marked on the listed items.

Express Mail No. (if applicable) EL624352520

Date: Aug. 29, 2000

By:

Helen M. Hare
Helen M. Hare

EL624352520

Approved for use through 09/30/2000. OMB 0651-0032
 Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

for FY 2000

Patent fees are subject to annual revision.
 Small Entity payments must be supported by a small entity statement,
 otherwise large entity fees must be paid. See Forms PTO/SB/09-12.
 See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT

(\$1390⁰⁰)

Complete if Known

Application Number

Filing Date

First Named Inventor

MARIANI ET AL.

Examiner Name

Group / Art Unit

Attorney Docket No.

MSI - 57945

METHOD OF PAYMENT (check one)

1. ☐ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number

12-0769

Deposit Account Name

LEE S. HAYES, PLLC

☒ Charge Any Additional Fee Required
 Under 37 CFR §§ 1.16 and 1.17

2. ☒ Payment Enclosed:

☒ Check ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Small Entity

Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Description	Fee Paid
101 690	201 345		Utility filing fee	690
106 310	206 155		Design filing fee	
107 480	207 240		Plant filing fee	
108 690	208 345		Reissue filing fee	
114 150	214 75		Provisional filing fee	

SUBTOTAL (1) (\$)

2. EXTRA CLAIM FEES

Total Claims	Extra Claims	Fee from below	Fee Paid
35	-20** = 15	18	270
8	-3** = 5	78	390
Multiple Dependent			

**or number previously paid, if greater; For Reissues, see below

Large Entity Small Entity

Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Description	Fee Paid
103 18	203 9		Claims in excess of 20	
102 78	202 39		Independent claims in excess of 3	
104 260	204 130		Multiple dependent claim, if not paid	
109 78	209 39		** Reissue independent claims over original patent	
110 18	210 9		** Reissue claims in excess of 20 and over original patent	

SUBTOTAL (2) (\$)

(\$660⁰⁰)

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Small Entity

Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Description	Fee Paid
105 130	205 65		Surcharge - late filing fee or oath	
127 50	227 25		Surcharge - late provisional filing fee or cover sheet	
139 130	139 130		Non-English specification	
147 2,520	147 2,520		For filing a request for reexamination	
112 920*	112 920*		Requesting publication of SIR prior to Examiner action	
113 1,840*	113 1,840*		Requesting publication of SIR after Examiner action	
115 110	215 55		Extension for reply within first month	
116 380	216 190		Extension for reply within second month	
117 870	217 435		Extension for reply within third month	
118 1,360	218 680		Extension for reply within fourth month	
128 1,850	228 925		Extension for reply within fifth month	
119 300	219 150		Notice of Appeal	
120 300	220 150		Filing a brief in support of an appeal	
121 260	221 130		Request for oral hearing	
138 1,510	138 1,510		Petition to institute a public use proceeding	
140 110	240 55		Petition to revive - unavoidable	
141 1,210	241 605		Petition to revive - unintentional	
142 1,210	242 605		Utility issue fee (or reissue)	
143 430	243 215		Design issue fee	
144 580	244 290		Plant issue fee	
122 130	122 130		Petitions to the Commissioner	
123 50	123 50		Petitions related to provisional applications	
126 240	126 240		Submission of Information Disclosure Stmt	
581 40	581 40		Recording each patent assignment per property (times number of properties)	40
146 690	246 345		Filing a submission after final rejection (37 CFR § 1.129(a))	
149 690	249 345		For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify)

Other fee (specify)

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$)

(\$40⁰⁰)

SUBMITTED BY

Name (Print/Type)

James R. Banowsky

Registration No.
(Attorney/Agent)

37,773

Complete (if applicable)

Telephone

(509)324-9256

Signature

James R. Banowsky

Date

8/29/00

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

006200" 27/05/96

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Systems and Methods for Limiting Access To
Potentially Dangerous Code**

Inventor(s):

Rico Mariani
David M. Broman
Sanjeev K. Rajan
Kristi L. Cooper

ATTORNEY'S DOCKET NO. MS1-579US

00624352520

1 **TECHNICAL FIELD**

2 The systems and methods described herein relate to network security and,
3 more particularly, to securing web pages and software controls to prevent
4 unauthorized web pages from utilizing software controls on a client computer to
5 corrupt or misappropriate data on the client computer.

6
7 **BACKGROUND**

8 Website developers frequently utilize software controls to provide
9 specialized functionality to web applications. Generally, a software control
10 (hereinafter, "control") is defined as program instructions that manage data-
11 handling tasks. Controls are typically reusable software components in binary
12 form that can be plugged into other software components with relatively little
13 effort. For example, a stock ticker control may be used to add a live stock ticker to
14 a web page, or an animation control can be used to add animation features to a
15 web page.

16 Controls may be downloaded to a Client computer together with the web
17 pages that invoke them. Once a control is downloaded by a web page, it remains
18 on the Client computer. Subsequent execution of the web page will execute the
19 control without requiring the control to be downloaded again. However, other web
20 pages may also invoke the control, even though the control was not downloaded
21 with that web page. This invocation may even be accomplished without the user's
22 knowledge.

23 This can lead to exploitation of the control by an unauthorized user. The
24 unauthorized user may use the control for something other than its intended
25 function, or use the control function in a manner contrary to the intended use of

1 the control function. The results of such exploitation can be loss or corruption of
2 data, exposure of sensitive materials, or other security compromises.

3 As an example of how serious this exploitation can be, consider a user who
4 downloads a control that access banking software on the user's computer. The
5 user trusts the author of the control and the website, and uses the control according
6 to its intended function. But when the user has finished using the control, the user
7 may not even be aware that the control and its functionality remain on the user's
8 computer. Thereafter, a web page set up by a hacker and accessed by the user may
9 invoke the control and gain access to the user's banking software. The hacker may
10 then have the ability to write unauthorized checks on the user's account, transfer
11 funds electronically from the account, and so on.

12 To help combat this problem, signed controls have been developed. Signed
13 controls contain a digital signature that uniquely identifies the author of the
14 control. When the signed control is accessed, the control is authenticated by the
15 downloading computer. Once authenticated, a determination is made as to
16 whether the author of the control is an authorized source for controls. If so, the
17 control may be invoked. However, this verification is only made when the control
18 is initially downloaded. Once the user downloads the control, the control may be
19 invoked by any other application without authorization from the user.

20 In addition to signed controls, the notion of trusted sites has been utilized
21 whereby a user may confidently use a control downloaded from certain user-
22 identified sites. Again, however, the problem remains that once a user has
23 authorized the download of a control, the user can no longer safeguard against
24 unauthorized use of that control.

1 Some operating systems, such as the WINDOWS family of operating
2 systems produced by MICROSOFT CORPORATION, provide a feature whereby
3 a control writer can specifically mark a control as being "safe" to avoid having to
4 perform additional steps each time the control is used. A control can only be
5 marked as safe if no other web site could possibly use the control in an unsafe
6 manner. Once the control is marked as safe, it can be invoked without further
7 precautionary measures being taken.

8 It is desirable to mark a control as safe so that a computer user can be
9 confident that the control can be downloaded without causing harm to the user's
10 computer. However, many valuable controls that can be safely invoked cannot be
11 marked as safe because they do not satisfy the requirement that they cannot be
12 used in an unsafe manner. These controls must be marked as "unsafe" even
13 though they can be invoked in a safe manner. This is problematic in that a user
14 may not download such a control simply because it is marked as unsafe, since the
15 user does not know the exact reason that the control has been marked as unsafe.
16 Such an unsafe designation may cause unnecessary apprehension and
17 inconvenience to the user.

18 The implementations described herein overcome this disadvantage and
19 allow a control writer to mark a control as safe, since malicious web pages will be
20 prevented from invoking the safe control in an unsafe manner.
21
22
23
24
25

1 SUMMARY

2 Methods and systems are described herein that allow a control to be
3 invoked only by an authenticated and authorized application. A web page is
4 described that invokes a software control that has been previously downloaded to a
5 Client computer, or which is contained in the web page to be downloaded by the
6 Client computer. The web page is digitally signed by the author so that the Client
7 computer can ensure that the control is being invoked by a trusted source. A
8 confirmation module located in a web browser on the Client computer or in the
9 control itself authenticates the digital signature and confirms whether the web
10 page is authorized by the Client computer to invoke the control. If the web page is
11 authenticated and authorized, then the Client computer allows the web page to
12 invoke the control.

13 The described implementations solve the problems presented above,
14 because an invoking application is authenticated and authorized each time the
15 control is invoked rather than only when the control is downloaded. Therefore, an
16 unauthorized user cannot gain access to a control previously downloaded onto the
17 Client computer.

1 **BRIEF DESCRIPTION OF THE DRAWINGS**

2 A more complete understanding of exemplary methods and arrangements
3 of the present invention may be had by reference to the following detailed
4 description when taken in conjunction with the accompanying drawings wherein:

5 Fig. 1 is a diagram of an exemplary computer system on which the
6 described embodiments may be implemented.

7 Fig. 2 is a block diagram of a server computer and a client computer
8 according to an implementation described herein.

9 Fig. 3 is a flow diagram of a process to prevent use of a control by an
10 unauthorized application.

11
12 **DETAILED DESCRIPTION**

13 The invention is illustrated in the drawings as being implemented in a
14 suitable computing environment. Although not required, the invention will be
15 described in the general context of computer-executable instructions, such as
16 program modules, to be executed by a computing device, such as a personal
17 computer or a hand-held computer or electronic device. Generally, program
18 modules include routines, programs, objects, components, data structures, etc. that
19 perform particular tasks or implement particular abstract data types. Moreover,
20 those skilled in the art will appreciate that the invention may be practiced with
21 other computer system configurations, including multi-processor systems,
22 microprocessor-based or programmable consumer electronics, network PCs,
23 minicomputers, mainframe computers, and the like. The invention may also be
24 practiced in distributed computing environments where tasks are performed by
25 remote processing devices that are linked through a communications network. In

1 a distributed computing environment, program modules may be located in both
2 local and remote memory storage devices.

3 4 **Exemplary Computer Environment**

5 The various components and functionality described herein are
6 implemented with a number of individual computers. Fig. 1 shows components of
7 typical example of such a computer, referred by to reference numeral 100. The
8 components shown in Fig. 1 are only examples, and are not intended to suggest
9 any limitation as to the scope of the functionality of the invention; the invention is
10 not necessarily dependent on the features shown in Fig. 1.

11 Generally, various different general purpose or special purpose computing
12 system configurations can be used. Examples of well known computing systems,
13 environments, and/or configurations that may be suitable for use with the
14 invention include, but are not limited to, personal computers, server computers,
15 hand-held or laptop devices, multiprocessor systems, microprocessor-based
16 systems, set top boxes, programmable consumer electronics, network PCs,
17 minicomputers, mainframe computers, distributed computing environments that
18 include any of the above systems or devices, and the like.

19 The functionality of the computers is embodied in many cases by
20 computer-executable instructions, such as program modules, that are executed by
21 the computers. Generally, program modules include routines, programs, objects,
22 components, data structures, etc. that perform particular tasks or implement
23 particular abstract data types. Tasks might also be performed by remote
24 processing devices that are linked through a communications network. In a
25

distributed computing environment, program modules may be located in both local and remote computer storage media.

The instructions and/or program modules are stored at different times in the various computer-readable media that are either part of the computer or that can be read by the computer. Programs are typically distributed, for example, on floppy disks, CD-ROMs, DVD, or some form of communication media such as a modulated signal. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable media when such media contain instructions programs, and/or modules for implementing the steps described below in conjunction with a microprocessor or other data processors. The invention also includes the computer itself when programmed according to the methods and techniques described below.

For purposes of illustration, programs and other executable program components such as the operating system are illustrated herein as discrete blocks, although it is recognized that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.

With reference to Fig. 1, the components of computer 100 may include, but are not limited to, a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120. The system bus 121 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not

1 limitation, such architectures include Industry Standard Architecture (ISA) bus,
2 Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video
3 Electronics Standards Association (VESA) local bus, and Peripheral Component
4 Interconnect (PCI) bus also known as the Mezzanine bus.

5 Computer 100 typically includes a variety of computer-readable media.
6 Computer-readable media can be any available media that can be accessed by
7 computer 100 and includes both volatile and nonvolatile media, removable and
8 non-removable media. By way of example, and not limitation, computer-readable
9 media may comprise computer storage media and communication media.
10 "Computer storage media" includes both volatile and nonvolatile, removable and
11 non-removable media implemented in any method or technology for storage of
12 information such as computer-readable instructions, data structures, program
13 modules, or other data. Computer storage media includes, but is not limited to,
14 RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM,
15 digital versatile disks (DVD) or other optical disk storage, magnetic cassettes,
16 magnetic tape, magnetic disk storage or other magnetic storage devices, or any
17 other medium which can be used to store the desired information and which can be
18 accessed by computer 110. Communication media typically embodies computer-
19 readable instructions, data structures, program modules or other data in a
20 modulated data signal such as a carrier wave or other transport mechanism and
21 includes any information delivery media. The term "modulated data signal"
22 means a signal that has one or more of its characteristics set or changed in such a
23 manner as to encode information in the signal. By way of example, and not
24 limitation, communication media includes wired media such as a wired network or
25 direct-wired connection and wireless media such as acoustic, RF, infrared and

1 other wireless media. Combinations of any of the above should also be included
2 within the scope of computer readable media.

3 The system memory 130 includes computer storage media in the form of
4 volatile and/or nonvolatile memory such as read only memory (ROM) 131 and
5 random access memory (RAM) 132. A basic input/output system 133 (BIOS),
6 containing the basic routines that help to transfer information between elements
7 within computer 100, such as during start-up, is typically stored in ROM 131.
8 RAM 132 typically contains data and/or program modules that are immediately
9 accessible to and/or presently being operated on by processing unit 120. By way
10 of example, and not limitation, Fig. 1 illustrates operating system 134, application
11 programs 135, other program modules 136, and program data 137.

12 The computer 100 may also include other removable/non-removable,
13 volatile/nonvolatile computer storage media. By way of example only, Fig. 1
14 illustrates a hard disk drive 141 that reads from or writes to non-removable,
15 nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to
16 a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that
17 reads from or writes to a removable, nonvolatile optical disk 156 such as a CD
18 ROM or other optical media. Other removable/non-removable,
19 volatile/nonvolatile computer storage media that can be used in the exemplary
20 operating environment include, but are not limited to, magnetic tape cassettes,
21 flash memory cards, digital versatile disks, digital video tape, solid state RAM,
22 solid state ROM, and the like. The hard disk drive 141 is typically connected to
23 the system bus 121 through an non-removable memory interface such as interface
24 140, and magnetic disk drive 151 and optical disk drive 155 are typically
25

1 connected to the system bus 121 by a removable memory interface such as
2 interface 150.

3 The drives and their associated computer storage media discussed above
4 and illustrated in Fig. 1 provide storage of computer-readable instructions, data
5 structures, program modules, and other data for computer 100. In Fig. 1, for
6 example, hard disk drive 141 is illustrated as storing operating system 144,
7 application programs 145, other program modules 146, and program data 147.
8 Note that these components can either be the same as or different from operating
9 system 134, application programs 135, other program modules 136, and program
10 data 137. Operating system 144, application programs 145, other program
11 modules 146, and program data 147 are given different numbers here to illustrate
12 that, at a minimum, they are different copies. A user may enter commands and
13 information into the computer 100 through input devices such as a keyboard 162
14 and pointing device 161, commonly referred to as a mouse, trackball, or touch
15 pad. Other input devices (not shown) may include a microphone, joystick, game
16 pad, satellite dish, scanner, or the like. These and other input devices are often
17 connected to the processing unit 120 through a user input interface 160 that is
18 coupled to the system bus, but may be connected by other interface and bus
19 structures, such as a parallel port, game port, or a universal serial bus (USB). A
20 monitor 191 or other type of display device is also connected to the system bus
21 121 via an interface, such as a video interface 190. In addition to the monitor,
22 computers may also include other peripheral output devices such as speakers 197
23 and printer 196, which may be connected through an output peripheral interface
24 195.
25

1 The computer may operate in a networked environment using logical
2 connections to one or more remote computers, such as a remote computer 180.
3 The remote computer 180 may be a personal computer, a server, a router, a
4 network PC, a peer device or other common network node, and typically includes
5 many or all of the elements described above relative to computer 100, although
6 only a memory storage device 181 has been illustrated in Fig. 1. The logical
7 connections depicted in Fig. 1 include a local area network (LAN) 171 and a wide
8 area network (WAN) 173, but may also include other networks. Such networking
9 environments are commonplace in offices, enterprise-wide computer networks,
10 intranets, and the Internet.

11 When used in a LAN networking environment, the computer 100 is
12 connected to the LAN 171 through a network interface or adapter 170. When used
13 in a WAN networking environment, the computer 100 typically includes a modem
14 172 or other means for establishing communications over the WAN 173, such as
15 the Internet. The modem 172, which may be internal or external, may be
16 connected to the system bus 121 via the user input interface 160, or other
17 appropriate mechanism. In a networked environment, program modules depicted
18 relative to the computer 100, or portions thereof, may be stored in the remote
19 memory storage device. By way of example, and not limitation, Fig. 1 illustrates
20 remote application programs 185 as residing on memory device 181. It will be
21 appreciated that the network connections shown are exemplary and other means of
22 establishing a communications link between the computers may be used.

23 Fig. 2 is a block diagram of a Server-Client system 200 in accordance with
24 the implementations described herein. The system 200 includes a Server computer
25 202 and a Client computer 204. The Server computer 202 has a processor 206 and

1 memory 208. The memory 208 stores a page generator 210 for generating web
2 pages, including a web page 212 shown in the memory 208. A page delivery
3 module 214 in the memory 208 delivers the web page 212 to the Client computer
4 204 via a network (not shown).

5 The web page 212 contains executable script 216 and a control object 218,
6 which is invoked by the script 216 when the script 216 is executed on the
7 processor 206. A confirmation module 220 is included in the control object 218.
8 As will be discussed in greater detail below, the confirmation module 220 is
9 transmitted to the Client computer 204 with the control object 218 where it
10 authenticates any web page that attempts to invoke the control object 218 and
11 determines if an authenticated source is authorized to invoke the control object
12 218.

13 A digital signature module 222 is stored in the memory 208 of the Server
14 computer 202. The digital signature module 222 is configured to digitally sign the
15 web page 212 using any method known in the art. When the web page 212 is
16 digitally signed, a digital signature 226 is attached to the web page 212. The
17 digital signature 226 enables the Client computer 204 to authenticate the source of
18 the web page 212.

19 Depending on the implementation, the digital signature module 222 may
20 sign each web page generated by the page generator 210, or the digital signature
21 module 222 may only sign web pages that invoke a control. Regardless of the
22 implementation used in the present example, the web page 212 is digitally signed
23 with the digital signature 226 because the web page 212 contains the control
24 object 218 which is invoked by the web page 212.

1 The control object 218 is a reusable software component that conforms to a
2 standard, such as the COM (common object model) standard. The control object
3 218 may be used in a variety of containers, such as a Visual Basic program, a C++
4 program, an HTML web page, etc. The control object 218, when executed,
5 performs a function within the Client computer 204. This function may include,
6 but is not limited to, accessing data, manipulating data, providing animation,
7 displaying objects, etc.

8 The Client computer 204 includes a processor 227 and memory 228. A
9 web browser 230 is stored in the memory 228 and executes on the processor 227.
10 The web browser 230 enables the Client computer 204 to access the web page 212
11 on the server 202. As shown in Fig. 2, a copy of the web page 212 (designated as
12 web page 212') has been downloaded to the Client computer 204 and is stored in
13 the memory 228. The downloaded web page 212' includes a script 216' (a copy
14 of the script 216) and a control object 218' (a copy of the control object 218). A
15 copy of the confirmation module 218 (designated as confirmation module 218')
16 has been downloaded with the web page 212' and is a part of the control object
17 218'. The web page 212' is digitally signed with a digital signature 226' that was
18 downloaded with the web page 212'.

19 Fig. 3 is a flow diagram of a method to prevent execution of the control
20 object 218' by an unauthorized web page. For this discussion, continuing
21 reference will be made to the elements shown in Fig. 2.

22 At step 300, the web browser 230 on the Client computer 204 requests a
23 download of the web page 212 from the Server computer 202. If the web page
24 212 includes script 216 that invokes a control object ("Yes" branch, step 302),
25 then the digital signature module 222 on the Server computer 202 digitally signs

1 the web page 212 by attaching the digital signature 226 to the web page 212 at
2 step 304. The signed web page 212 is delivered to the Client computer 202 at step
3 306. If the web page 212 does not invoke a control object ("No" branch, step
4 302), the web page 212 is delivered to the Client computer 204 at step 306 without
5 a digital signature.

6 It is noted that step 302 is an optional step. If step 302 is not included in
7 the process, the digital signature module 222 will compute and attach a digital
8 signature to every web page that is downloaded from the Server computer 202.
9 The selected implementation depends on which implementation requires lower
10 requirements of server resources.

11 At step 308, the Client computer 204 receives the web page 212, 212' from
12 the Server computer 202. On many systems, a user of the Client computer 204
13 will be notified at this point if the user wishes to download the web page 212
14 having the control object 218. For purposes of the present discussion, it is
15 assumed that the user downloads the control object 218 with the web page 212.

16 If a web page or other application attempts to invoke the control object
17 218' on the Client computer 204 ("Yes" branch, step 310), the confirmation
18 module 220' authenticates the source of the web page 212' at step 312. The
19 confirmation module 220' determines from the digital signature 226' if the web
20 page 212' is from a source the web page 212' purports to come from. The exact
21 method of doing this is well known in the art.

22 If the confirmation module 220' determines that the web page 212' has
23 come from the source indicated by the web page 212', the confirmation module
24 220' then determines if the source is an authorized source at step 314. This can be
25 done in several ways. The author of the control object 218' may include a list of

sources that the author trusts to invoke the control object 218', or the user may be prompted at some point by the control object 218' to enter sources which the user trusts to invoke the control object 218' safely, or a list of trusted sites may be stored in the memory of the Client computer 204, etc. With any such implementation, the control object 218' checks the name of the source against one or more source names to determine if the source is authorized to invoke the control object 218'.

It is also noted that, in another implementation, the steps performed by the confirmation module 220' may be performed by the web browser 230 or by a module located in the web browser 230. In such an implementation, when the web page 212' attempts to invoke the control object 218', the web browser 230 will detect or be notified of the event and will attempt to authenticate and authorize the source of the web page 212'.

If the confirmation module 220' determines that the web page 212' has come from an authenticated and authorized source (the Server computer 202 in this example), then the control object 218' is executed at step 318. If the source cannot be authenticated ("No" branch, step 312) or if the source is not authorized to invoke the control object 218' ("No" branch, step 314), then the control object 218' will not be executed.

1 **Conclusion**

2 Control objects embedded in web pages are powerful tools that give a
3 programmer free access to a user's computer. The implementations described
4 provide a user with a way to prevent control objects from being executed by
5 unauthorized users. In this way, the user is assured of the source of the control
6 object and, if the user trusts the source, the user can confidently allow the control
7 object to be invoked.

8 A user is also assured that once a control object is downloaded to the user's
9 computer, it cannot be invoked by a web page or other application from a source
10 other than the source of the web page or application that originally included the
11 control object.

12 Although the implementation described herein have been described in
13 language specific to structural features and/or methodological steps, it is to be
14 understood that the invention defined in the appended claims is not necessarily
15 limited to the specific features or steps described. Rather, the specific features and
16 steps are disclosed as preferred implementations.

1 **CLAIMS**

2 1. A method, comprising:
3 associating a digital signature with a web page; and
4 delivering the web page to an electronic device capable of authenticating
5 the digital signature and executing at least a portion of the web page after the
6 digital signature is authenticated.

7
8 2. The method as recited in claim 1, wherein the associating further
9 comprises attaching the digital signature to the web page.

10
11 3. The method as recited in claim 1, further comprising:
12 determining if the web page includes code to invoke a control object; and
13 deriving the digital signature and associating the digital signature with the
14 web page only if the web page includes code to invoke a control object.

15
16 4. The method as recited in claim 1, wherein the web page includes a
17 confirmation module that is used by the electronic device to authenticate the
18 digital signature.

19
20 5. The method as recited in claim 1, wherein the web page contains
21 script that, when executed, invokes executable code that is executed on the
22 electronic device executing the web page.

23
24 6. The method as recited in claim 1, wherein the web page is generated
25 in an active server page (ASP) environment.

1
2 7. A method, comprising:
3 receiving a web page from a server, the web page containing executable
4 script that, when executed, invokes a control object, the web page having a
5 segment that uniquely identifies a source of the web page;
6 authenticating the source of the web page; and
7 displaying the web page and invoking the control object if the web page is
8 authenticated.

9
10 8. The method as recited in claim 7, further comprising:
11 determining if the source of the web page is authorized to invoke the
12 control object; and
13 displaying the web page only if the source of the web page is authorized to
14 invoke the control object.

15
16 9. The method as recited in claim 7, wherein the authenticating further
17 comprises authenticating the source of the web page to identify the source of the
18 web page.

19
20 10. The method as recited in claim 7, further comprising:
21 designating one or more authorized sources from which a web page that
22 invokes a control object may be received; and
23 executing script contained in the web page only if authenticating the source
24 of the web page indicates that the web page was received from an authorized
25 source.

1 **16.** The system as recited in claim 14, wherein the confirmation module
2 is included in a browser of the electronic device.

3
4 **17.** A system, comprising:
5 a web browser configured to access a web page having a digital signature;
6 a processor configured to execute script contained in the web page;
7 an executable control object that may be invoked by the script in the web
8 page and is executable on the processor;
9 a confirmation module configured to authenticate the digital signature; and
10 wherein the confirmation module is called when the control object is
11 invoked by the script, the control object executing only if the confirmation module
12 authenticates the digital signature.

13
14 **18.** The system as recited in claim 17, wherein the confirmation module
15 is called by the control object.

16
17 **19.** The system as recited in claim 17, wherein the confirmation module
18 is included in the control object.

19
20 **20.** The system as recited in claim 17, wherein the confirmation module
21 is included in the web browser.

1 **21.** The system as recited in claim 17, wherein the confirmation module
2 is further configured to determine if the web page comes from a source that is
3 authorized to invoke the control object and the control object is invoked only if the
4 source of the web page is authorized to invoke the control object.

5
6 **22.** The system as recited in claim 17, wherein the confirmation module
7 is called by the web page prior to the web page invoking the control object.

8
9 **23.** The system as recited in claim 17, wherein the digital signature
10 module is not invoked if the web page does not have a digital signature.

11
12 **24.** A web page contained on a computer-readable medium, comprising:
13 computer-executable script that, when executed on a computing device,
14 invokes an executable control object on the computing device; and
15 a digital signature uniquely identifying an author of the web page.

16
17 **25.** The web page as recited in claim 24, wherein the digital signature is
18 appended to the contents of the web page.

19
20 **26.** The web page as recited in claim 24, further comprising the
21 executable control object.

1
2 **27.** A web browser contained on a computer-readable medium of a
3 client computer, comprising computer-executable instructions that, when executed
4 by the client computer, perform the following:

5 determining if a web page contains instructions to invoke a control object;
6 authenticating the web page using a digital signature; and
7 invoking the control object if the source of the web page is authenticated.
8

9 **28.** The web browser as recited in claim 27, further comprising:
10 determining if the web page contains executable script to invoke a control
11 object; and

12 wherein the authenticating the web page further comprises authenticating
13 the web page only if the web page contains executable script to invoke a control
14 object.
15

16 **29.** The web browser as recited in claim 27, further comprising:
17 determining if the web page contains a digital signature; and
18 wherein the authenticating the web page further comprises authenticating
19 the web page only if the web page contains a digital signature.
20

21 **30.** The web browser as recited in claim 27, wherein the control object
22 is not invoked if the web page does not include a digital signature.
23
24
25

1 **31.** The web browser as recited in claim 27, further comprising
2 instructions to determine if an authenticated web page comes from a source that is
3 authorized to invoke the control object.

4
5 **32.** A control object stored in a computer-readable medium, comprising
6 computer-executable instructions that, when executed on a computer, perform the
7 following:

8 authenticating a web page that invokes the control object; and
9 executing a data-handling task on the computer if the web page is
10 determined to be authentic.

11
12 **33.** The control object as recited in claim 32, wherein the web page is
13 authenticated utilizing a digital signature attached to the web page.

14
15 **34.** The control object as recited in claim 32, further comprising
16 instructions to determine if a source of the web page is authorized to invoke the
17 data-handling task prior to executing the data-handling task.

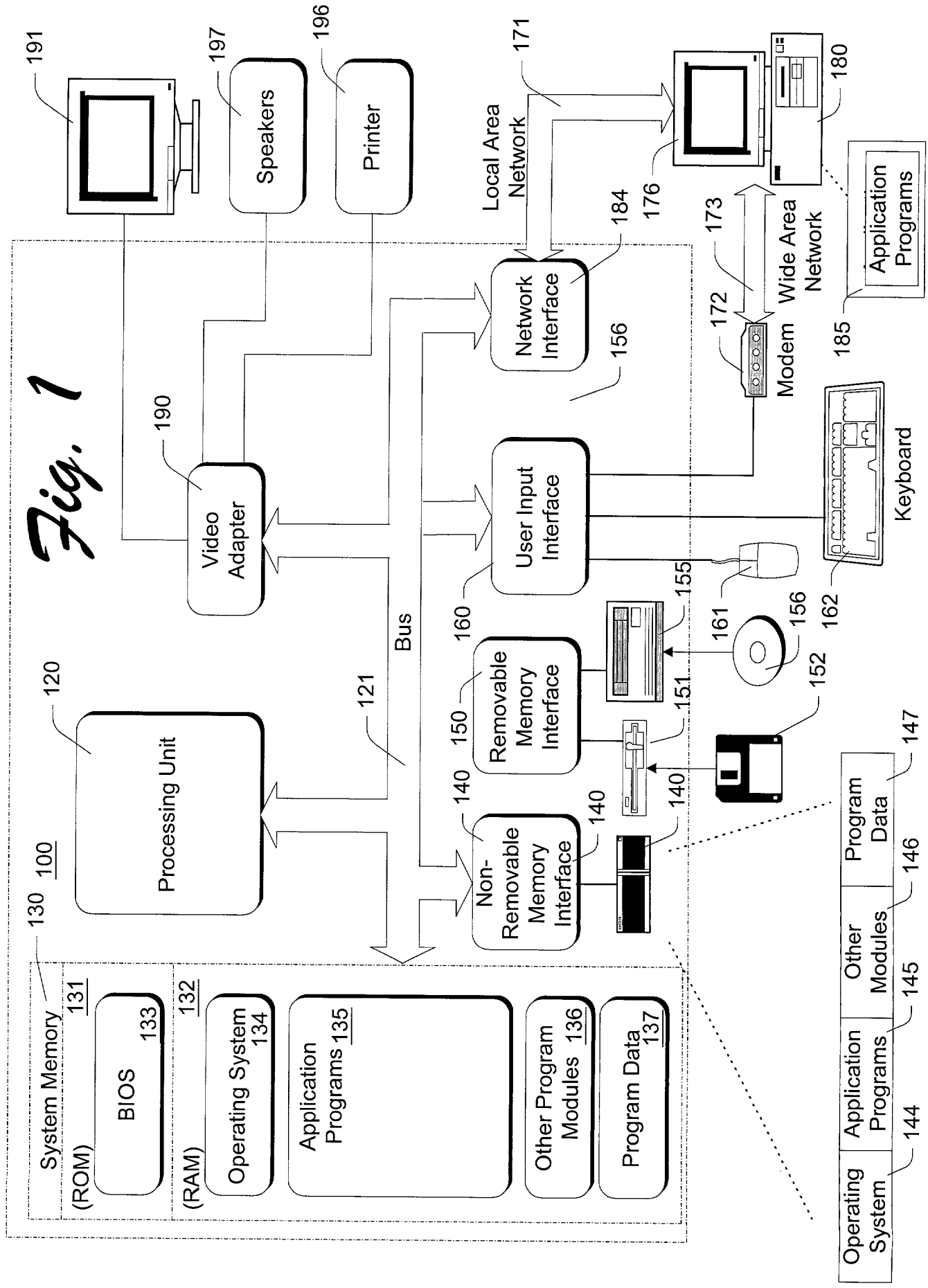
18
19 **35.** A modulated data signal having data fields encoded thereon
20 transmitted over a communication channel, comprising:

21 a first data field containing data representing a web page; and
22 a second data field containing data representing a digital signature derived
23 from the web page represented by the first data field.

1 **ABSTRACT**

2 Systems, methods and data structures are described for attaching a digital
3 signature to a web page and authenticating the digital signature before allowing
4 the web page to invoke a software control on a computer that has downloaded the
5 web page. Unauthorized users cannot gain access to a control on a computer
6 through a web page that is downloaded to the computer, if the source of the web
7 page or application cannot be authenticated or is not a trusted source.

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25



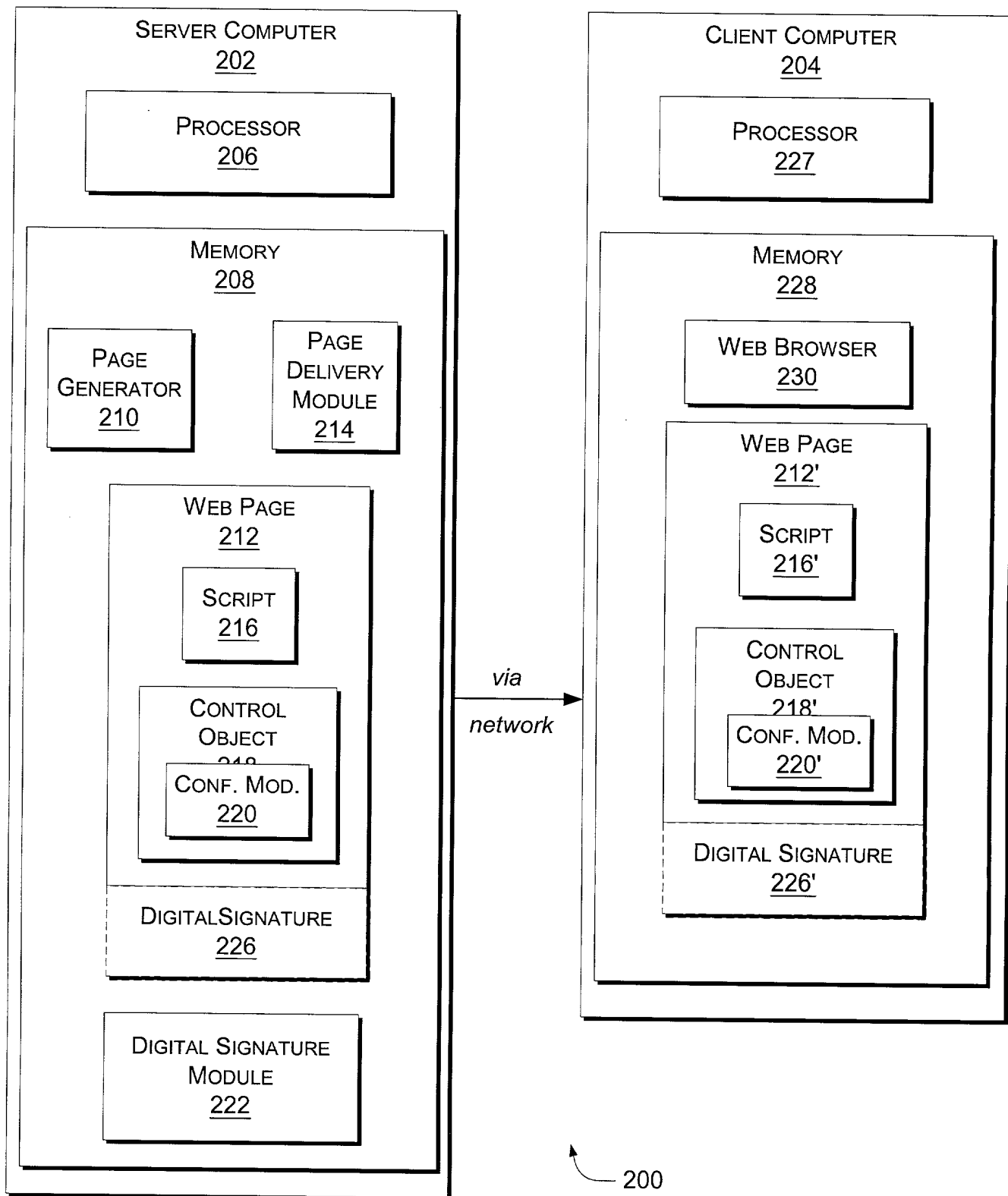


Fig. 2

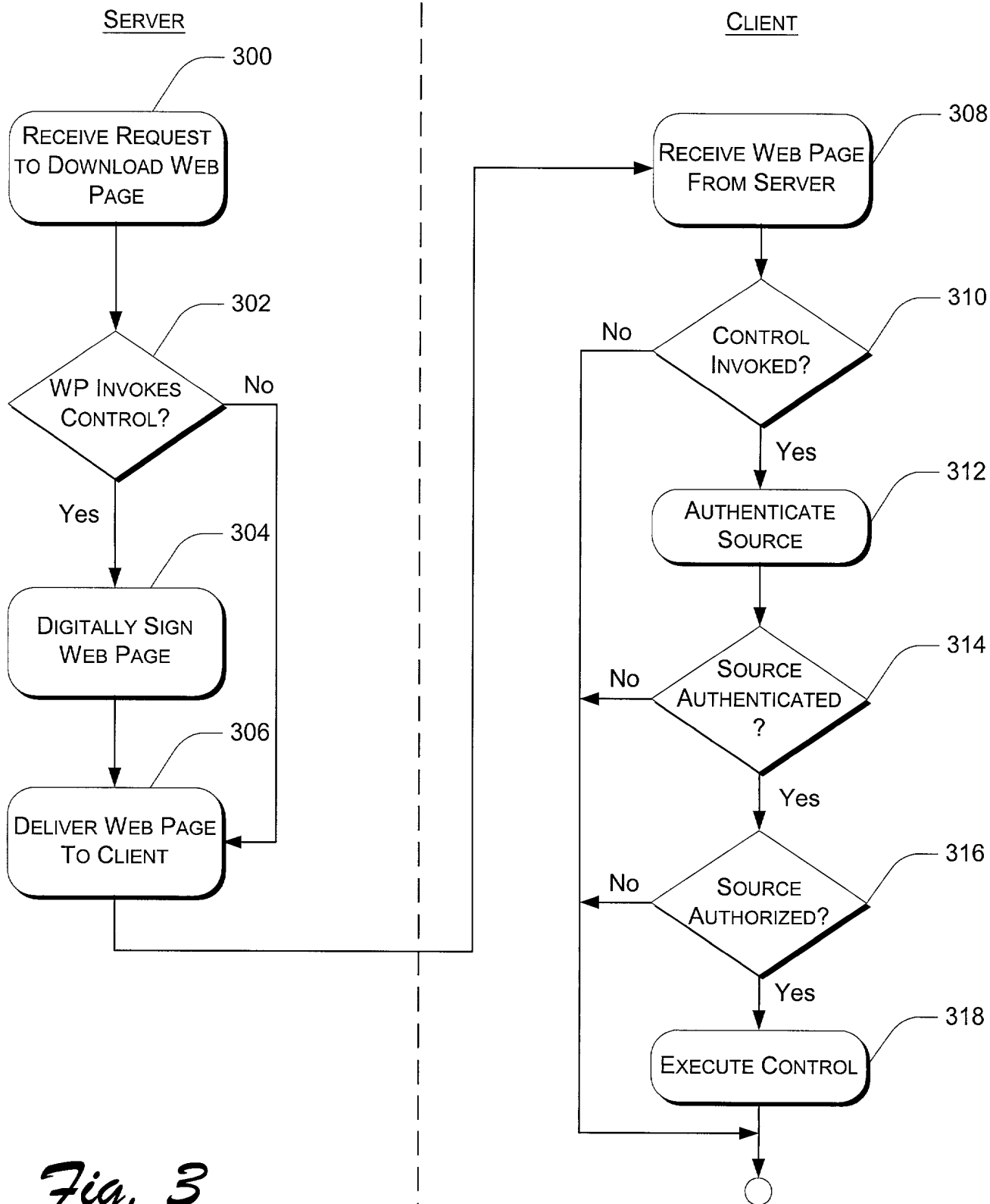


Fig. 3

1 **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2 Inventorship..... Mariani et al.
 3 Applicant Microsoft Corporation
 4 Attorney's Docket No. MS1-579US
 Title: Systems and Methods for Limiting Access to Potentially Dangerous Code

5 **DECLARATION FOR PATENT APPLICATION**

6 As a below named inventor, I hereby declare that:

7 My residence, post office address and citizenship are as stated below next to
 8 my name.

9 I believe I am the original, first and sole inventor (if only one name is listed
 10 below) or an original, first and joint inventor (if plural names are listed below) of the
 11 subject matter which is claimed and for which a patent is sought on the invention
 12 entitled "Systems and Methods for Limiting Access to Potentially Dangerous Code,"
 the specification of which is attached hereto.

13 I have reviewed and understand the content of the above-identified
 14 specification, including the claims.

15 I acknowledge the duty to disclose information which is material to the
 16 examination of this application in accordance with Title 37, Code of Federal
 17 Regulations, § 1.56(a).

18 **PRIOR FOREIGN APPLICATIONS:** no applications for foreign patents or
 19 inventor's certificates have been filed prior to the date of execution of this
 20 declaration.

21 **Power of Attorney**

22 I appoint the following attorneys to prosecute this application and transact all
 23 future business in the Patent and Trademark Office connected with this application:
 24 Lewis C. Lee, Reg. No. 34,656; Daniel L. Hayes, Reg. No. 34,618; Allan T.
 25

1 Sponseller, Reg. 38,318; Steven R. Sponseller, Reg. No. 39,384; James R.
2 Banowsky, Reg. No. 37,773; Lance R. Sadler, Reg. No. 38,605; Michael A. Proksch,
3 Reg. No. 43,021; Thomas A. Jolly, Reg. No. 39,241; David A. Morasch, Reg. No.
4 42,905; Kasey C. Christie, Reg. No. 40,559; Nathan R. Rieth, Reg. No. 44,302;
5 Brian G. Hart, Reg. No. 44,421; Katie E. Sako, Reg. No. 32,628 and Daniel D.
6 Crouse, Reg. No. 32,022.

7 Send correspondence to: LEE & HAYES, PLLC, 421 W. Riverside Avenue,
8 Suite 500, Spokane, Washington, 99201. Direct telephone calls to: James R.
9 Banowsky (509) 324-9256.

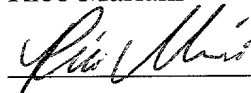
10
11 All statements made herein of my own knowledge are true and that all
12 statements made on information and belief are believed to be true; and further that
13 these statements were made with the knowledge that willful false statements and the
14 like so made are punishable by fine or imprisonment, or both, under Section 1001 of
15 Title 18 of the United States Code and that such willful false statement may
16 jeopardize the validity of the application or any patent issued therefrom.

17
18 * * * * *

19 Full name of inventor:

Rico Mariani

20 Inventor's Signature



Date: 8/24/2000

21 Residence:

Kirkland, WA

22 Citizenship:

Canada

23 Post Office Address:

13433 NE 104th Street
Kirkland, WA 98033

Full name of inventor:

David M. Broman

Inventor's Signature

David M. Broman

Date: 8-24-00

Residence:

Redmond, WA

Citizenship:

USA

Post Office Address:

18103 NE 28th Street
Redmond, WA 98052

Full name of inventor:

Sanjeev K. Rajan

Inventor's Signature

Sanjeev K. Rajan

Date: 08/24/00

Residence:

Kirkland, WA

Citizenship:

India

Post Office Address:

4315 Lake Washington Blvd. #3208
Kirkland, WA 98033

Full name of inventor:

Kristi L. Cooper

Inventor's Signature

Kristi L. Cooper

Date: 8/24/00

Residence:

Bellevue, WA

Citizenship:

USA

Post Office Address:

14777 NE 50th Pl. Apt. L6
Bellevue, WA 98007

005280" 27.05960